REMARKS

In view of the above amendments and the following discussion, the Applicants submit that none of the claims now pending in the application are anticipated under the provisions of 35 U.S.C. § 102. Thus, the Applicants believe that all of these claims are now in allowable form.

I. REJECTION OF CLAIMS 1-11 UNDER 35 U.S.C. §102

The Examiner has rejected claims 1-11 in the Office Action under 35 U.S.C. § 102 as being anticipated by Murakawa (US Publication Number 2001/0020273, Published September 6, 2001, hereinafter referred to as "Murakawa"). The Applicants respectfully traverse the rejection.

Murakawa teaches a method of virtual private network communications in security gateway apparatus and security gateway apparatus using the same. Maurakawa teaches a PC client that sends an IP packet to a security gateway (see Murakawa, Paragraph [0071]). The security gateway encapsulates the IP packet and sent to a second PC client via VPN (see *Id.* at [0072] - [0075]).

The Examiner's attention is directed to the fact that Murakawa fails to teach, show or suggest a method of sending a packet from a first IPSec client to a second IPSec client comprising the steps of, receiving at a non-proprietary format tunneling protocol server from the first IPsec client an IPsec packet wrapped in the non-proprietary tunneling format and creating a non-proprietary format tunneling protocol tunnel, as positively claimed by the Applicants' independent claims. For example, Applicants' independent claim 1 positively recites:

> 1. A method of sending a packet from a first IPSec client to a second IPSec client, comprising the steps of:
> receiving at a non-proprietary format tunneling protocol server from the first IPsec client an IPsec packet wrapped in the non-proprietary tunneling format;
> creating a non-proprietary format tunneling protocol tunnel to the second IPsec client through the non-proprietary format tunneling protocol server;
> establishing a security association between the first and second IPSec clients via the non-proprietary format tunneling protocol server;

transmitting the packet through the non-proprietary format tunneling protocol tunnel to the second IPSec client whereby the packet remains unaffected by any address translation or firewall traversal that may occur during transmission. (Emphasis Added)

7. A method of sending a packet from a first IPSec client to a second IPSec client comprising the steps of:

receiving an IPsec packet wrapped in a Layer 2 Tunneling Protocol (L2TP) format packet from the first IPsec client at a L2TP server;

setting up an L2TP tunnel from the L2TP server to the second IPsec client;

establishing a security association between the first and second IPSec clients via the L2TP server; and

transmitting the packet through the L2TP tunnel to the second IPSec client whereby the packet remains unaffected by any address translation or firewall traversal that may occur during transmission. (Emphasis added)

The Applicants' invention teaches a method of sending a packet from a first IPSec client to a second IPSec client via a non-proprietary format tunneling protocol server. Specifically, Applicants teach that the non-proprietary format tunneling protocol server (e.g., L2TP server) receives from the first IPsec client an IPsec packet wrapped in the non-proprietary tunneling format. In turn, the non-proprietary format tunneling protocol server creates a non-proprietary format tunneling protocol tunnel (e.g., L2TP tunnel) to the second IPsec client. For example, the IPsec gateway wraps each IPsec packet in a L2TP format for transmission to the L2TP network server (see Applicants' Specification, Page 4, Lines 1-4). Then the L2TP server creates a tunnel to a second IPsec client and transmits the wrapped data IPsec packet via the tunnel (see *Id.* at Lines 5-9). As such, the combination of wrapping the IPsec packet in a non-proprietary tunneling format and creating a tunnel via non-proprietary format tunneling protocol server allows IPsec packets to bypass devices, such as a Network Address Translation (NAT) device, thereby, avoiding transmission difficulties that arise from sending IPsec packets through such devices (see *Id.* at Page 2, Lines 13-20).

Murakawa clearly fails to anticipate the Applicants' invention in several respects. First, Murakawa fails to teach a non-proprietary format tunneling protocol server that is capable of receiving from a first IPsec client an IPsec packet wrapped in the non-proprietary tunneling format. Murakawa only teaches having a first client PC 101, a

security gateway 203, and a second client PC 106 (see Murakawa, Figure 1). Specifically, the security gateway taught by Murakawa and the non-proprietary format tunneling protocol server taught by the Applicants are not the same. Murakawa teaches that the security gateway receives an IP data packet that is not encapsulated (see Murakawa, Paragraph [0072]; Figure 1). In contrast, the non-proprietary format tunneling protocol server taught by the Applicants' invention receives an IPsec packet that is already wrapped in the non-proprietary tunneling format. In other words, at best, Murakawa's security gateway 203 can be interpreted as an IPsec client, but it is absolutely not a non-proprietary format tunneling protocol server.

Moreover, Murakawa completely fails to teach, show or suggest the step of creating a non-proprietary format tunneling protocol tunnel via the non-proprietary format tunneling protocol server (see Applicants' Specification, Page 2, Lines 13-20). In contrast, Murakawa teaches establishing a single VPN connection and transmitting the encapsulated packet through said single VPN connection (see Murakawa, Paragraph [0070] and [0075]). Murakawa is completely devoid of any teaching of a tunnel via a non-proprietary format tunneling protocol server. As such, the Applicants respectfully submit that independent claims 1 and 7 are clearly not anticipated by Murakawa.

Furthermore, dependent claims 2-6 and 8-11 depend, either directly or indirectly, from claims 1 and 7 and recite additional limitations. As such, and for the exact same reason set forth above, the Applicants submit that claims 2-6 and 8-11 are also patentable and not anticipated by Murakawa. As such, the Applicants respectfully request the rejection be withdrawn.

Conclusion

Thus, the Applicants submit that all of these claims now fully satisfy the requirement of 35 U.S.C. §102. Consequently, the Applicants believe that all these claims are presently in condition for allowance. Accordingly, both reconsideration of this application and its swift passage to issue are earnestly solicited.

If, however, the Examiner believes that there are any unresolved issues requiring the issuance of a final action in any of the claims now pending in the application, it is requested that the Examiner telephone Mr. Kin-Wah Tong, Esq. at (732) 530-9404 so that appropriate arrangements can be made for resolving such issues as expeditiously as possible.

Respectfully submitted,

10/7/05

Patterson & Sheridan, LLP
595 Shrewsbury Avenue
Shrewsbury, New Jersey 07702

Kin-Wah Tong, Attorney
Reg. No. 39,400
(732) 530-9404